NVLAP®	DEPARTMENT OF COMMERCE National Institute of Standards and Technology National Voluntary Laboratory Accreditation Program	**ISSUE DATE:** October 2, 2001
	LAB BULLETIN	**NUMBER:** LB-5-2001
		LAP: ITST CCT

SUBJECT: WRITTEN PROCEDURES

This bulletin applies to the Information Technology Security Testing, Common Criteria Testing Program.

NIST Handbook 150:2001, paragraph 4.2.1 states:

> "The laboratory shall establish, implement and maintain a quality system appropriate to the scope of its activities. The laboratory shall document its policies, systems, programs, procedures and instructions to the extent necessary to assure the quality of the test and/or calibration results. The system's documentation shall be communicated to, understood by, available to, and implemented by the appropriate personnel."

The ISO 9000 hierarchy of written documents is 1) policy, 2) procedure, 3) instruction, and 4) record. ISO 8402:1994, *Quality management and quality assurance—Vocabulary,* 1.3, *procedure,* Note 3 states: "A written or documented procedure usually contains the purposes and scope of an activity; what shall be done and by whom; when, where and how it shall be done; what materials, equipment and documents shall be used; and how it shall be controlled and recorded."

The details that identify the steps to accomplish a task may be removed from a "Procedure" document to one or more "Instruction" documents. An instruction gives step-by-step details about how specific tasks are performed. While a procedure tells what to do, an instruction can tell how to do it. Instructions can include operating manuals for devices, checklists of steps to be taken, and customization of procedures for each evaluation.

Written procedures and instructions provide for consistency within the laboratory over time and among evaluation teams. The written procedures and instructions along with the records generated by each activity also allow internal and external auditors to verify that the quality system is being properly used.

W. Edwards Deming described the following cycle of events: say what you do, do what you say, record that you have done it, audit for compliance and effectiveness, feed back and continuously improve.

For the NVLAP Information Technology Security Testing program for Common Criteria Testing, each applicant and accredited laboratory must have written and implemented procedures. Implementation is used here to mean that the appropriate quality system and technical documents have been written, experts and expertise obtained, training conducted, activity conducted, activity audited, and management review conducted. Procedures are an integral part of the laboratory quality system and must be included in all aspects of the laboratory

operation. A laboratory must implement all of the procedures (listed below or not) that are required to meet the accreditation requirements of NIST Handbook 150:2001 and NIST Handbook 150-20 (Draft Version 1.1, July 27, 1999; and later). Failure to have implemented procedures may lead to suspension of NVLAP accreditation.

General Procedures (required, but not limited to)

The general procedures listed below are required and must be implemented before accreditation can be granted.

a) Procedure for internal audits and management review.

b) Procedure for writing and implementing procedures.

c) Procedure for writing and implementing instructions.

d) Procedure on staff training and individual development plans.

e) Procedure on contract review.

f) Procedures for staff members who work at home and at alternate work sites outside the laboratory (e.g., telecommuting).

g) Procedure on referencing NVLAP accreditation and use of the NVLAP logo. (It is recommended that use of the NIAP and CC logos be controlled.)

Program-Specific Procedures (required, but not limited to)

The program-specific procedures listed below must be implemented before the activity is undertaken, e.g., procedure for writing Common Methodology (CEM) work-unit level instructions before an evaluation is conducted.

a) Procedure for writing a Work Plan for an evaluation.

b) Procedure on selecting the members of an evaluation team.

c) Procedure on writing an Evaluation Technical Report (ETR).

d) Procedure on writing an Observation Report (OR).

e) Procedure for conducting an evaluation at a client's site (if the laboratory offers such services).

f) Procedures for conducting evaluations for: ST, PP, and EAL levels 1, 2, 3, and 4 for specific technologies (e.g., firewalls, operating systems, biometric devices).

g) Procedure for vulnerability analysis.

h) Procedure for conducting independent testing.

i) Procedure for requesting and incorporating CC interpretations.

j) Procedure for working with NIAP or other validators during an evaluation.

k) Procedure for records and record keeping for evaluations. There must be enough evaluation evidence in the records so that an independent body, including NVLAP and CCEVS, can 1) determine the evaluation work actually performed for each work unit and 2) concur with the verdict. Records include evaluator notebooks, records relating to the product, work-unit level records, client-site records, etc.

l) Procedure for writing Common Methodology (CEM) work-unit-level instructions to describe how the work unit will be performed for a given PP or TOE evaluation. Not all work units will require such instructions. Examples of work units requiring specific instructions for TOE evaluations include:

- ADV_FSP.1-4, ADV_FSP.2-4
- ADV_FSP.1-5, ADV_FSP.2-5
- ADV_LLD.1-7
- ADV_HLD.2-11
- AGD_ADM.1-7
- ATE_IND.2-4
- ATE_COV.2-3

Questions or comments concerning this bulletin should be directed to Jeffrey Horlick at <jeffrey.horlick@nist.gov>.